Published in *Proceedings of the Twenty-Ninth Southeastern Symposium on System Theory*, IEEE Control Society, New York, 1997.

Secure Optical Communications Using Wavelength Tunable Optical Filters

Ron J. Pieper, John P. Powers and Phillip E.Pace
Department of Electrical and Computer Engineering
Naval Postgraduate School, Monterey, California

Abstract

This report will present several conceptual designs for all-optical implementations to enhance the security of optical communications links. The method takes advantage of technology which uses the wavelength selective filtering properties of electronically tunable high finesse Fabry-Perot interferometers(FPIs. For the application under consideration the FPI would physically separate from a broad band (e.g., > 20 nm) optical source, such as superluminescent LED, a narrow band (e.g., < 0.1 nm) of wavelengths and the latter would be modulated with the information signal of interest. The modulated optical signal is combined with the unmodulated part of the broadband signal prior to transmission. The decoding process at the receiver would require an identical FPI tuned to the same narrow band of wavelengths in order to selectively extract the modulated narrowband signal carrying the information transmitted. Robustness of the security is enhanced by the electronic tunability of the FPIs which could potentially lead to a wavelength-hopped transmission and tracking communication system.

1 Identification of the Problem

The problem of transmittance and reception of sensitive information is not unlike the allegorical game of the cat and mouse. As soon as one or more technological developments are established that can increase the security of a communication link, there will the action-reaction pressure to engineer countermeasures that would thwart these same developments. In such an environment the concept of sufficient security becomes difficult to justify. The communications community has to date embraced two widely different and well-known techniques in order to add security to the process of transmittal of information. One of these techniques, data encryption, can be traced back to the Romans who used simple but efficient methods. In more modern times data encryption has become much more sophisticated and is generally based on the mathematical discipline generally referred to as information theory[1]. The second method known as spread-spectrum, has been applied in communication systems design as early as the 1940s. These spread spectrum systems are primarily lumped into one of two subcategories, direct sequence systems and frequency hopped systems [2]. Both techniques lead to a general spreading of the transmitted RF spectrum. The first subcategory uses direct modulation of the information with a high speed pseudo-random code. The receiver has a lock on the pseudo-random code and can correctly decode the information. A by-product of the direct sequence modulation is a widening of the transmitted spectrum. The second method, frequency hopping, has the carrier literally hopping from channel to channel across a band of frequencies.

The advent of the laser in the early 1960s and the developments of semiconductor-based LEDs and laser diodes in the 1970s and 1980s have directly led to design and fielding of modern optical communication systems. Although optical fiber has undoubtedly become the predominant option for long-distance transmission of information, there is a significant contingent of research and development work still being done on free-space optical communications especially for applications relating to nonterrestial satellite communications. See for example any of the recent SPIE proceedings on free-space laser communication technologies[3]. For deep-space applications it is projected[4] that by the year 2000 optical technology will have advantages over RF technology on issues such as aperture size, terminal weight and recurring cost.

Until recently, one of the great advantages of optical fiber communication systems has been the difficulty presented to external parties wishing to intercept or inject information. However it is now possible to purchase commercial field fiber splicers which can break and resplice an optical fiber communication system in minutes [5]. It is not difficult to imagine

how such hardware could be retrofitted to allow third parties to break into a fiber optic communication systems without a noticeable change in the transmission characteristics from the viewpoint of sender and receiver. Presumably any informed third party,(i.e., one who has access to the transmission protocols and has knowledge on how to extract and interpret the data) could in a detectionless manner compromise the security of the line.

By the very nature of free-space communications, whether RF or optical, the lack of spatial confinement of the signal gives undisputed and legal access to any party who intercepts some part of the signal. For free-space optical transmissions the signal can be spatially directed toward some intended receiver using a laser source and beam collimating optical components. Nonetheless, there will be unavoidable diffraction limiting spreading of a laser optical beam which, over the typical long distances associated with satellite communications, would be expected to create a spatial optical field waist that greatly exceeds the narrow receiving window of the intended target. The scenario that is possible here is not unlike the case of the optical fiber. An informed third party could pick off part of the optical signal and compromise the security of the link.

Herein lies the motivation for establishing another potential layer of security which can be introduced independent of the other more established layers of security, i.e., data encryption and spread spectrum (RF domain). As illustrated in Fig 1. the logical level for this layer to be developed would be in the optical domain. The concepts to be introduced in the optical domain will to a significant degree parallel those concepts used in spread spectrum in the RF domain.

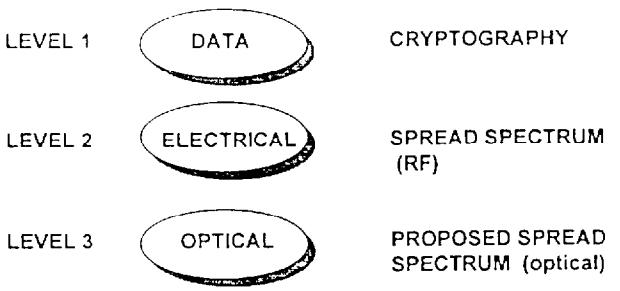


Figure 1: Domain interpretation for secure communications

The advantage of the integration of the optical wavelength hopped security scheme is, in fact, more significant than just another layer of security. One application niche where this is particularly evident in the real-time transmission of color images. Take for example a 60 Hz frame rate, having $1024 \times 1024 \times 8$ bit resolution and a lossless compression of 3. With these numbers the required data is 0.5 G bit/sec. Although this is a fraction of the bandwidth capabilities of single-mode optical fiber systems, [6] commercially available encryption systems are limited to 1/10 of this rate (e.g., Cylink's 45 M b/sec Inforguard for ATM system [7]) On the other hand, the proposed wavelength-hopped optical system is operationally independent of the data rate. Therefore, the proposed optical system could be used to transmit and receive the high data rate bit stream, without limiting throughput, and still add a significant measure of security.

There has been recent interest in a novel optical scheme for creating a data-secure system using the quantum effects of photons [8, 9]. This scheme has been tested experimentally and the results indicate that single photon detector noise was introducing noise at the 6% level. The residual errors were electronically filtered out using more conventional methods. However, this again restricts the throughput. In addition the quantum nature of the measurement requires a highly sensitive but noisy avalanche photodiode [8]. The advantage in this method, as pointed out by the investigators, is that this method is essentially 100% free of detectionless tampering. The proposed wavelength-hopped scheme for enhancing the security will not exhibit this attractive property. however because it is based on nonquantum effects, it will be less sensitive to noise and therefore it will not exhibit residual errors which require throughput limiting error correction.

2 Background

The Fabry-Perot filter has the property that it can selectively pass a very narrow band of wavelengths and reject (or more precisely reflect) the remaining wavelengths. What makes these filters so useful is the option of controlling the filtering properties electronically. There are some definitions generally applicable to these filters which can be explained with the aid of Figs. 2 and 3. First, the free spectral range, $\Delta\sigma$, is the frequency spacing between Fabry-Perot resonant frequencies. For light at normal incidence these resonant frequencies follow the rule:

$$\nu_m = \frac{mc}{2nd} \qquad m = \text{positive integer} \qquad (1)$$

where n is the index of refraction, d is the mirror spacing and c is the vacuum speed of light. Therefore the free spectral range is given by

$$\Delta\sigma = \frac{c}{2d}. \qquad (2)$$

The relationship between FWHM, $\Delta\xi$, of the resonances and the free spectral range is defined by the finesse of the filter,

$$F = \frac{\Delta\sigma}{\Delta\xi}. \quad (3)$$

The optical filters considered here are assumed to be lossless. Mathematically this is represented by the power conservation rule:

$$R^2 + T^2 = 1 \quad (4)$$

where R and T are respectively the reflection and transmission amplitude coefficients. This condition can be predicted from analysis [10] and has been observed experimentally [11].

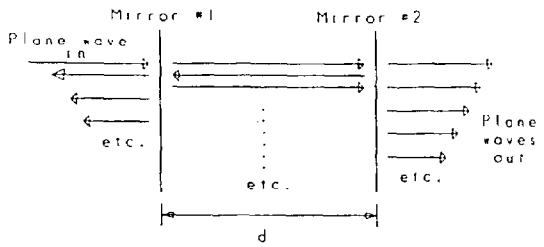


Figure 2: The Fabry-Perot interferometer

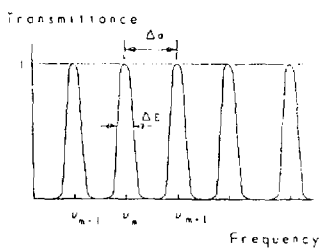


Figure 3: Transmissivity vs. frequency for the Fabry-Perot interferometer

3 Commercially available tunable optical filters

A partial list of vendors, supplying both bulk and free space electronically tunable optical filters, appears in the list of references. [12,13,14,15]. One common feature of these commercially available "off-the shelf" tunable filters is that these devices have in all cases been designed to minimize the percentage of back reflection that is coupled into the return path. For most optical communications applications such as wavelength division multiplexing the reflected power can create interference problems if it is not properly extinguished. However, for the concept being proposed the combination of the reflected part of the optical spectrum with the information-bearing modulated optical signal can provide significant advantages. For later reference in the discussion, a system which is designed to take advantage of the back reflected component will be referred to as type A. The use of commercial FPIs does not completely restrict the application of the concept but it does limit the ability of the design, type B, to hide the signal in the spectrum. Therefore in order to develop the design with the maximum possible security features, within the framework of the basic concept, it presently appears that a custom tunable filter would need to be constructed. Alternatively a laboratory tunable filter could be built [11].

4 Free-space design

A free-space, type-A optical communication system employing the proposed concept is represented in Fig 4 As shown on this figure, a laser diode at the transmitter supplies a narrow collimated optical beam with a requirement that the output optical spectral bandwidth is high compared with the FWHM of FPI 1 and preferably less than the free spectral range of the FPI. Various neutral density filters (ND1-ND3) have been included for technical reasons relating to diagnostics and reliability of the system. Also this design calls for the use of an optical isolator. The beam splitters 1 and 2 rout the reflected optical signal to the other side of an optical modulator (e.g., an AO cell). The unmodulated reflected broadband optical signal will be recombined with the modulated narrow-band optical signal selected by FPI 1.

Part of the combined optical signal falls on FPI 2 which will be tuned through electronic control to the same wavelength as at the transmitting side. Due to proper tuning of FPI 2 that part of the incident radiation which has been electro-optically modulated will be transmitted and the remaining unmodulated optical radiation (> 99%) will be rejected. The S/N advantage gained by having a FPI at the receiver matched to FPI 1 can then be established through comparison of the diagnostic wideband signal obtained at detector D 2 (which bypasses FPI 2) and the narrow-band signal measured at D 1. These signals can then be viewed on the oscilloscope or a spectrum analyzer allowing an establishment of the signal to noise ratio.By adding a *self-tracking* design for locking the FPIs in synchronization then creates a

wavelength-hopped communication system.

5 Optical-fiber designs

Figure 5a represents the transmitter in an all optical-fiber type-A design. Among the required optical components include a circulator, an electro-optic or acoutsto-optic modulator and a 2x2 coupler. In this design the back reflection signal is routed via the optical isolator into the feed-forward optical fiber path which is physically attached to a piezoelectric pusher. The piezoelectric pusher shown is electronically driven by broadband white noise voltage source, which creates pressure disturbance on the fiber leading to intensity modulation on the feed-forward optical spectrum. The pseudo-modulation enhances the security of the optical transmission by creating false modulation signal on all optical wavelengths except, of course, the spectral slice that is passed by the Fabry Perot tunable filter. The two signals are combined at the transmitter. Unfortunately, as previously noted, commercially available electronically controlled optical filters will not work here.

Figure 5b represents an all-optical-fiber type B design for the transmitter. It is assumed that a commercially available optical tunable filter is used. In this design a 1x2 splitter supplants the circulator. In this case the back reflection of the optical filter is not being utilized. One major disadvantage of this design is that the feed-forward optical signal contains the same narrow band of optical wavelengths that is under FPI control. Because of this, pseudo noise modulation, if applied as in the previous case, would also create noise interference in the final composite signal in the information band. Although the design, is not as robust to countermeasures as the previous design it should still make third-party detection more difficult. The only viable measure which could thwart this scheme would be for the third party to capture the entire range of signals on the detector and attempt to extract the signal by stripping out the DC and amplifying; however, for this to work several problems would need to be addressed. The slice of modulated signal might for example represent a fraction of power of one 50th or less of the entire band. The narrowness of the slice would be expected to limit the actual power in the desired band on detector and therefore require shot-noise limited detection. In this regime the noise power is proportional to the total optical power falling on the detector and therefore the shot-noise for the third party receiver will be substantially higher and, consequently suffer a significant S/N disadvantage. Second, it is observed that the power level within any narrow band of the entire source spectrum will generally depend on the wavelength. Therefore some variations in the detected information-bearing signal would automatically occur as the wavelength was hopped. This could be predicted and accounted for at the receiver used in the overall communication link design but could not be predicted by any technique available to a third party. The lack of predictability in the signal level for the third-party detection process again supports the claim that the type B design has limited security enhancing features.

6 Conclusion

In this report several data independent, all optical schemes for adding security to confidential transmissions are discussed. These schemes could be applied to either free-space transmissions or optical fiber transmissions. The most effective scheme would require a custom-built electronically controlled optical tunable filter which allows for the use of the back reflected optical spectrum.

7 References

[1] R. W. Hamming, *Coding and Information Theory*, Prentice Hall, 1986.

[2] R. C. Dixon, "Why spread spectrum," *IEEE Communications Society's Tutorials in Modern Communications*, V. B. Lawrence, J. l. LoCicero, and L. B. Milstein, eds., pp. 317–322.,1980

[3] Special issue on "Free-Space Laser Communication Technologies VIII," *SPIE Proceedings*, Vol 2699, San Jose January 1996

[4] R. G. Marshalek et al., "System-level comparison for space-to-space and space-to-ground links circa 2000," *SPIE Proceedings*, Vol 2699,pp134-145, January 1996

[5] Optical Fiber Conference, San Jose, CA, Feb. 28, 1996.

[6] J. P. Powers, *An Introduction to Fiber Optic Systems*, Second Edition, Richard D. Irwin, 1997

[7] Cylink Corp., Sunnyvale, CA.

[8] P. D. Townsend, "Secure key distribution based on quantum cryptography," *Electronics Letters*, Vol. 30, No. 10, pp. 809–811, May 1994.

[9] C. H. Bennett, G. Brassard, and A. Ekert, "Quantum Cryptography," *Scientific American*, pp. 50–57, Oct. 1992.

[10] A. Yariv, *Optical Electronics*, HRW 1985

[11] S. Ezekiel,"Optics: Multiple Beam Interference," part 5 of the MIT series on *Video Demonstrations in Lasers and Optics*

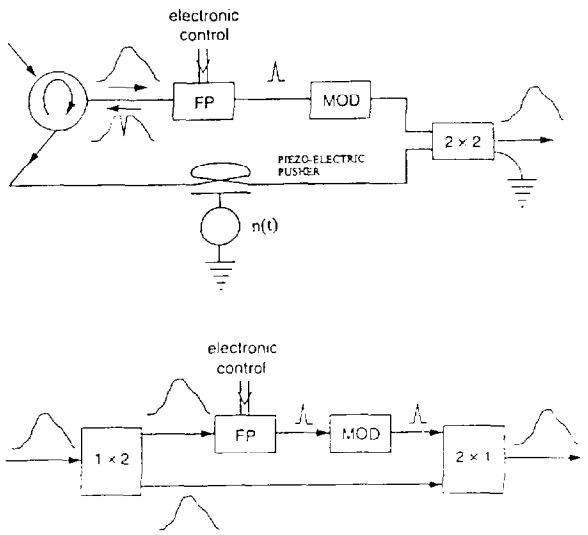
[12] Meadolark Optics, Longmont, CO.

[13] Burleigh Instruments Inc., Fisher, NY, (716) 924-9072.

[14] Santec USA Co., Holmdel N.J.

[15] Queensgate Intstruments Ltd., Ascot, U.K.

Figure 5: Optical fiber designs for transmitters



a) Type A (upper) and b) Type B (lower)

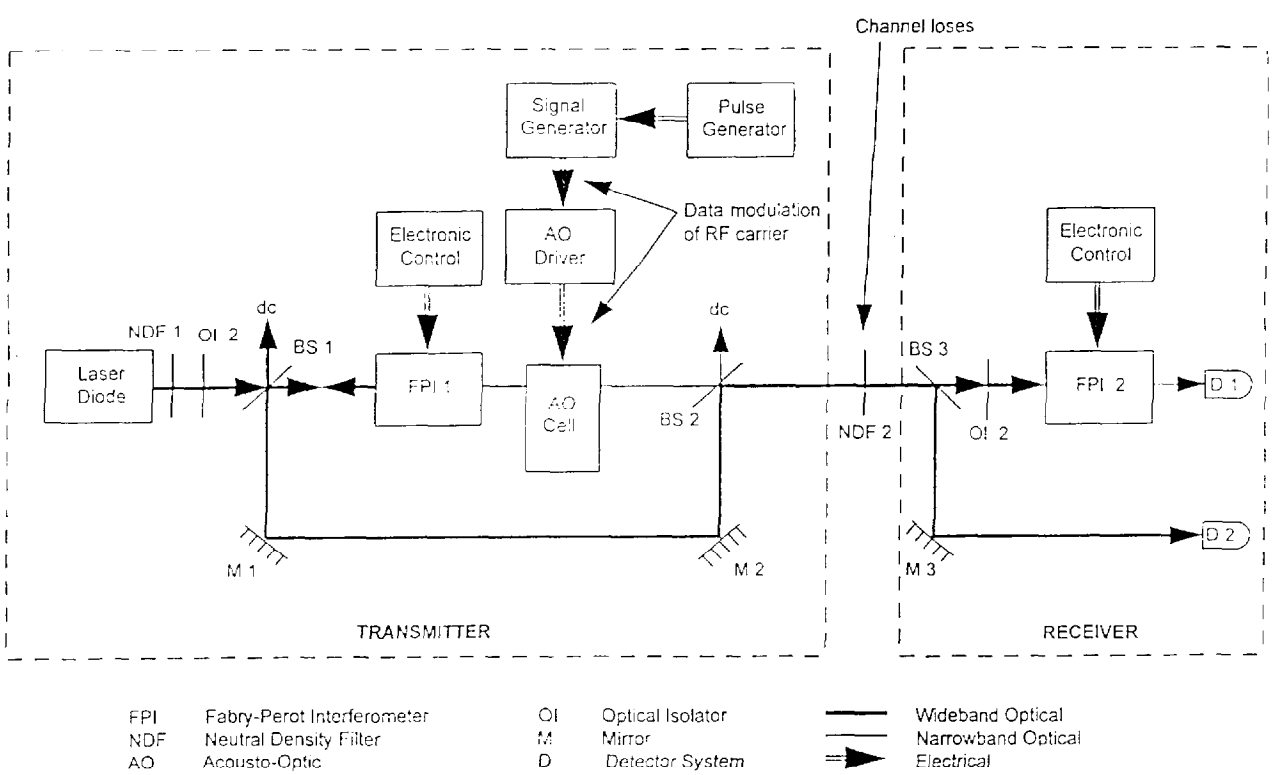


Figure 4: Free space test design